PRO AND IND

MAX STEINBERG // NOVEMBER 15, 2024

All rings are commutative unless otherwise specified.

1. Introduction

You may have heard of *p-adic* numbers. You might know what they are, or you might not. Today, we will give a brief definition of the p-adic integers in the context of a more general construction called *completion* (specifically *pro-completion*, as opposed to *ind-completion*).

Problem 1. (Review.) Describe all prime ideals of $\mathbb{Z}$.

Given an ideal $\mathfrak{p}$ of a ring R, we can form the *quotient ring* $R/\mathfrak{p}$. Recall that an ideal $\mathfrak{p}$ is prime if and only if $R/\mathfrak{p}$ is an integral domain. (This is not that bad to prove by showing that a ring is an integral domain if and only if (0) is prime, and using ideal transfer.) Also recall that we can *square* an ideal $\mathfrak{p}^2 = \langle p \cdot q | p, q \in \mathfrak{p} \rangle$ (by $\langle \dots \rangle$ we mean the ideal *generated* by these elements). We define $\mathfrak{p}^n$ similarly (including $\mathfrak{p}^0$ – what is this?).

Problem 2. Verify that $\mathfrak{p}^n$ is an ideal for any $n \geq 0$ and $\mathfrak{p} \subset R$ an ideal.

Problem 3. Show that there is a surjective map $R/\mathfrak{p}^n \to R/\mathfrak{p}^{n-1}$. *Hint: Third Isomorphism Theorem. What is* $(R/\mathfrak{p}^n)/(\mathfrak{p}^{n-1}/\mathfrak{p}^n)$*?*

Let's work in the integers for now. Since $\mathbb{Z}$ is a PID, we will write (n) to denote the ideal generated by n. Your answer to Problem 1 should help with this problem.

Problem 4. Show that there is a surjective map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ if and only if $m|n$.

Problem 5. Show that if $\mathfrak{p} = (n)$, then $\mathfrak{p}^k = (n^k)$ for $n \in \mathbb{Z}, k \geq 0$.

2. Limits

In Problem 3, we proved that the following diagramme forms an *inverse system*.

$$R/\mathfrak{p} \leftarrow R/\mathfrak{p}^2 \leftarrow R/\mathfrak{p}^3 \leftarrow \dots$$

(This is in opposition to a *direct system*, which would be a diagramme $A \to B \to C \to ....$) Formally, an inverse system requires a *partially ordered set* to be indexed by. In our case, we will use $\mathbb{N}$ to index our inverse system, which is totally ordered under $\leq$[1]. We will write f_i to denote the surjective map $R/\mathfrak{p}^i \to R/\mathfrak{p}^{i-1}$.

With an inverse system, we can take a *inverse limit*, also known as the *projective limit*:

$$\varprojlim_n R/\mathfrak{p}^n := \left\{ \vec{r} \in \prod_n R/\mathfrak{p}^n \;\middle|\; f(r_i) = r_{i-1} \right\}$$

In words, this is a collection of elements, one from each $R/\mathfrak{p}^i$, that are *consistent*: that is, if we send the i-th element through the map, we get the $i-1$-th element. Because our maps may not be injective (and in general will never be, because they are surjective), there are a lot of choices here!

Example 1. Let $R = \mathbb{Z}$ and $\mathfrak{p} = (p)$ for some prime $p \neq 0$. Then we write

$$\mathbb{Z}_p = \mathbb{Z}/p^\infty\mathbb{Z} := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

This is called the ring of *p-adic integers*. Let's describe the elements of this ring. Classically, p-adic integers are described as sums $\sum_0 a_i p^i$, where $0 \leq a_i \leq p$. We can represent this by $x_0 = a_0, x_1 = a_0 + a_1 p, \dots$.

Clearly given $\{x_0, x_1, \dots\}$ we can recover $\{a_0, a_1, \dots\}$ and thus $\sum_0 a_i p^i$. How else can we describe our data $\{x_0, x_1, \dots\}$? Well, we can say that $x_{i-1} \cong x_i \mod p^i$, since $x_{i-1} + a_i p^i = x_i$.

Problem 6. Prove that this description of the p-adic integers agrees with our definition $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. *Hint: $f_{i+1} : \mathbb{Z}/p^{i+1}\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ is also $x \mapsto x \mod p^i$, so our data can also be described as collections $\{x_0, x_1, \dots\}$, with $x_0 \in \mathbb{Z}/p\mathbb{Z}, x_1 \in \mathbb{Z}/p^2\mathbb{Z}, \dots$ (why?) and $f_{i+1}(x_i) = x_{i-1}$.*

Problem 7. Let $R = \mathbb{R}[t]$, the ring of real-coefficient polynomials in t. Describe $\varprojlim_n \mathbb{R}[t]/t^n\mathbb{R}[t]$. *Hint: use a similar approach to the p-adic integers.*
$R' = \varprojlim_n \mathbb{R}[t]/t^n\mathbb{R}[t]$ is called the *t-adic completion* of $\mathbb{R}[t]$.

[1] Literally, these are *sequential limits* because they operate over $\mathbb{N}$. A more general inverse limit can run over any partially ordered set, and is an example of a *cofiltered limit*, a limit indexed over a *cofiltered category*. A filtered category is a generalisation of a partially ordered set and a cofiltered category is simply the opposite category. We like cofiltered limits because they work very nicely with finite colimits (and dually filtered colimits work nicely with finite limits).

3. Profinite Groups

A group is called *profinite* if it is a *projective* limit (inverse limit) of *finite* groups. The classic example is the p-adic integers.

Problem 8. Is every profinite group infinite? Prove or give a counterexample.

Another important example of profinite groups is Galois groups. Given a field F and a Galois extension E/F, it is true that $\mathrm{Gal}(E/F)$ is *profinite*. Let $\{F_j\}$ be the collection of all fields such that $F \subset F_j \subset E$ and F_j/F is finite. Then

$$\mathrm{Gal}(E/F) = \varprojlim_j \mathrm{Gal}(F_j/F)$$

Thus, $\mathrm{Gal}(E/F)$ is profinite, as F_j/F is a finite extension and hence $\mathrm{Gal}(F_j/F)$ is finite. As the last topic in this short worksheet, we will prove that $\mathrm{Gal}(E/F) = \varprojlim_j \mathrm{Gal}(F_j/F)$. To do so, we will learn *pro-ind duality*.

Fix F a field, and $E/K/F$ extensions with E/F (and thus necessarily E/K and K/F) finite. The map $K \hookrightarrow F$ (the "hook" on this arrow meaps the map is injective) induces a map $\mathrm{Gal}(K/F) \leftarrow \mathrm{Gal}(E/F)$ (this is the quotient map by the subgroup $H \subset \mathrm{Gal}(E/F)$ that fixes K). Notice how the arrow is now reversed. If we call the map from $f : F \to K$, then we write $\mathrm{Gal}(f/F) : \mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$.

$$K \xrightarrow{\quad f \quad} E$$

$$\mathrm{Gal}(K/F) \xleftarrow[\mathrm{Gal}(f/F)]{} \mathrm{Gal}(E/F)$$

This means that $\mathrm{Gal}(-/F)$ is *contravariant*: it reverses maps. (It would be "covariant" if it didn't reverse maps.)

Consider a (potentially infinite) Galois extension E/F. Let $E = \bigcup_i F_i$, where each F_i/F is finite and $F_i \subset F_{i+1}$.

Problem 9. Prove that this is always possible. *Hint: you may use without proof that an infinite extension E/F is Galois if and only if $E = \bigcup_i E_i$ with E_i/F Galois. Prove that we can order the E_i in the way we want. The field compositum may help.*

Then

$$\mathrm{Gal}(E/F) = \mathrm{Gal}\left(\left(\bigcup_i F_i\right)/F\right)$$

by definition. We can write $F = F_0 \to F_1 \to F_2 \to \dots$ and $f_i : F_i \to F_{i+1}$, and this forms a *direct system*. Thus, we can take a *direct limit* (also called an injective limit, or inductive limit) $\varinjlim_i F_i = \bigsqcup_i F_i/\sim$, where $a \sim b$ if $f_i(a) = b$ or $f_i(b) = a$ for some i.

In words, $\varinjlim_j F_i$ is the union of all F_i where we delete duplicates.

Problem 10. Prove that if all f_i are injective, then $\varinjlim_j F_j = \bigcup_j F_j$.

Now, we have all the pieces we need to finish our proof.

$$\begin{aligned}\mathrm{Gal}(E/F) &= \mathrm{Gal}\left(\left(\bigcup_j F_j\right)/F\right)\\ &= \mathrm{Gal}((\varinjlim_j F_j)/F)\\ &= \varprojlim_i \mathrm{Gal}(F_i/F)\end{aligned}$$

Using *pro-ind duality*: because $\mathrm{Gal}(-/F)$ is contravariant, it sends

$$F_0 \to F_1 \to \dots$$

to

$$\mathrm{Gal}(F_0/F) \leftarrow \mathrm{Gal}(F_1/F) \leftarrow \dots$$

So our direct system becomes an inverse system. We don't know for sure that Gal sends our direct limit to an inverse limit though! For a contravariant functor, the property of sending direct limits to inverse limits is called *cocontinuity* and is a rather strong condition.

But in this case it is true![2] So our inductive limit (the *ind*) becomes a projective limit (the *pro*). So we've proved $\mathrm{Gal}(E/F) = \varprojlim_i \mathrm{Gal}(F_i/F)$ when $E = \bigcup_i F_i$.

[2]The Fundamental Theorem of Galois Theory states that subgroups of $\mathrm{Gal}(E/F)$ and subfields K with $E/K/F$ are in bijection. This is actually an equivalence of categories! The functor in one direction is $\mathrm{Gal}(-/F)$ and in the other way $E^{(-)}$ (the fixed points functor). These functors form a *adjunction*, with $\mathrm{Gal}(-/F)$ the left adjoint. It is a general theorem in category thoery that left adjoints are cocontinuous.